BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0063-2023-GTI220-N

INFORME TÉCNICO PREVIO - SERVICIO DE IMPLEMENTACION DE ACTUALIZACION DEL SOFTWARE PARA EL ACCESO A LAS CAJAS DE SEGURIDAD - SIX/TCL

1. NOMBRE DEL AREA:

Subgerencia de Servicios de Tecnologías de Información

2. RESPONSABLES DE LA EVALUACION:

Miguel Tejada Malaspina
Luis Diaz Vargas
Hernán Bohorquez Pérez

3. CARGOS:

Subgerente de Servicios de Tecnologías de Información
Jefe del Dpto. de Operaciones, Plataforma y Base de Datos
Especialista en Operaciones, Plataforma y Base de Datos

4. FECHA:

1 de marzo del 2023

5. JUSTIFICACIÓN

El BCRP, como parte de sus funciones relacionados a los Sistemas de Pagos, tiene implementado un sistema para atender las operaciones de alto valor denominado Sistema de Liquidación Bruta en Tiempo Real (Sistema LBTR). Está desplegado en una infraestructura de Servidor de Aplicaciones Oracle Weblogic 12c sobre Sistema Operativo Oracle Solaris 11 y tecnología de máquina virtual Java 7, utilizando el software de gestión de datos Oracle 12c configurado en alta disponibilidad. Este Sistema, considerado como un servicio crítico del banco, brinda los servicios de transferencias interbancarias de alto valor a las entidades que conforman el sistema financiero, de forma eficiente, segura y en tiempo real.

Actualmente el BCRP cuenta con la infraestructura tecnológica para el Sistema LBTR, donde el software SIX/TCL permite la integración de este sistema con los equipos de seguridad HSM.

Se requiere elevar el nivel de seguridad del Sistema LBTR, por ello se debe contratar el servicio de implementación de la actualización del software SIX/TCL, que consistirá en la instalación, configuración, pruebas y soporte técnico del software de integración del módulo de seguridad del Sistema LBTR y los equipos de seguridad HSM, que incorpore las siguientes características:

- Soporte para el firma y autenticación, cifrado/descifrado de mensajes con elmétodo de cifrado AES256.
- Soporte de LMK Keyblock

- Soporte del estándar JSON Web Token (JWT).
- Permitir la integración del Sistema LBTR con los equipos de seguridad HSM Thales Payshield 9000 y 10000, sin impactar la funcionalidad y el rendimiento dela solución, manteniendo las versiones de software base de la plataforma actual.

6. ALTERNATIVAS

Se ha considerado mantener el software SIX/TCL pues al ser un software de propiedad del BCRP en calidad de licencias perpetuas, y por ser un software estandarizado por ser parte importante de la plataforma tecnológica que soporta al Sistema de Pagos de Alto Valor – LBTR, específicamente en la parte de seguridad pues permite la integración del Sistema LBTR con las cajas de seguridad HSM. Esta integración brinda funciones de seguridad de alto nivel a las transferencias interbancarias que realizan las entidades del sistema financiero. Tiene funcionalidades que le permiten gestionar y trabajar con estándares de cifrado asimétricos, uso de firma digital y validación de mensajes, y encriptación simétrica para el cifrado de mensajes que soportan los equipos HSM. Por ello no se ha considerado la migración a otro software de características funcionales similares.

7. ANÁLISIS COMPARATIVO TÉCNICO

En base a las características técnicas (funcionales y no funcionales) y tomando en cuenta las necesidades técnicas actuales del Banco Central de Reserva del Perú, a continuación, se establecen las características del software SIX/TCL :

- Permite la integración multiplataforma, mediante el uso de librerías denominadas APIS's que se insertan en la aplicación o módulo de seguridad del Sistema LBTR, con los equipos de seguridad HSM.
- Permite llamados de alto nivel desde la aplicación de seguridad del LBTR que se traducen en llamados de bajo nivel invocando comandos propietarios de los equipos de seguridad HSM.
- Tiene funcionalidades que le permiten gestionar y trabajar con las características de encriptación asimétrica RSA, el uso de firma digital y validación de mensajes.
- Para el cifrado de data sensible utiliza la encriptación 3DES.

8. COSTO – BENEFICIO

COSTOS:

El servicio de implementación de la actualización del software SIX/TCL, que consistirá en la instalación, configuración, pruebas y soporte técnico del software de integración del módulo de seguridad del Sistema LBTR y los equipos de seguridad HSM, que incorpore las siguientes características de soporte para la firma y autenticación, cifrado/descifrado de mensajes con el método de cifrado AES256, soporte de LMK Keyblock, soporte del estándar JSON Web Token (JWT) y permitir la integración del Sistema LBTR con los equipos de seguridad HSM Thales Payshield 9000 y 10000, sin impactar la funcionalidad y el rendimiento de la solución,

manteniendo las versiones de software base de la plataforma actual, tiene un costo de S/. 134,375.57 incluido el IGV.

BENEFICIOS:

- Se contará con un esquema de cifrado de mejores características de seguridad, lo que permitirá dar un mayor nivel de protección y seguridad a las operaciones que se realicen en el Sistema LBTR.

- Se contará con un servicio de alto nivel de especialización y con el soporte especializado necesario para permitir una adecuada implementación del nuevo método de cifrado AES en la solución de seguridad del Sistema LBTR, con lo cual se podrá garantizar la continuidad operativa de este servicio.

9. CONCLUSIONES

Dada la necesidad de aumentar el nivel de seguridad en las transferencias entre bancos que se realizan a través del Sistema LBTR, y por ende actualizar el método de cifrado en el módulo de seguridad de este sistema y así implementar el método AES256, así como tener un soporte especializado para la adecuada implementación, sería necesario contar con un contrato servicio de implementación de la actualización del software SIX/TCL brindado por el fabricante o representante de la marca y comprende el soporte para el firma y autenticación, cifrado/descifrado de mensajes con el método de cifrado AES256, soporte de LMK Keyblock, soporte del estándar JSON Web Token (JWT) y permitir la integración del Sistema LBTR con los equipos de seguridad HSM Thales Payshield 9000 y 10000.

Lima, 27 de febrero de 2023

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Hernan Felipe BOHORQUEZ PEREZ
Especialista en Operaciones, Plataforma y Bases de Datos
Departamento de Operaciones, Plataforma y Bases de Datos

Luis Enrique DIAZ VARGAS
Jefe de Departamento de Operaciones, Plataforma y Bases de Datos
Departamento de Operaciones, Plataforma y Bases de Datos

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de Información
Subgerencia de Servicios de Tecnologías de Información

VISADO POR:

Silvia Elizabeth MEDINA MORENO
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración